AFFIDAVIT

I, Patrick Hanna, being duly sworn, depose and state as follows:

Introduction

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and currently assigned to the Burlington Resident Agency in Vermont. I have been an FBI Special Agent for 19 years. My duties as an FBI Special Agent include investigating violations of Title 18 of the United States Code as they pertain to corporate fraud, complex financial crimes, embezzlement, public corruption, money laundering and related white-collar crimes, as well as violent crimes and criminal enterprises. I have participated in investigations of criminal violations of various federal laws. I have executed search and arrest warrants, interviewed and interrogated subjects, witnesses, and victims, and conducted surveillance. In the course of these investigations, I have gained an understanding of current technology, to include computers and online accounts, cellular telephones and associated records and data, and have conducted analyses of the data related to such accounts and devices, for the purpose of solving and proving crimes.

2. I make this affidavit in support of an application for a search warrant authorizing the extraction and examination of data from an electronic device – a gray Apple iPhone 13 Pro Max (the "SUBJECT DEVICE"), currently in the custody of the FBI in Colchester, Vermont, as described in Attachment A – and the seizure of electronically stored information described in Attachment B.

3. On May 19, 2022, the federal grand jury sitting in Burlington, Vermont, charged Serhat Gumrukcu with conspiring with Berk Eratay and others between May 2017 and February 2018 to pay someone to murder Gregory Davis, whose body was discovered on January 7, 2018. As discussed below, there is probable cause to believe that Gumrukcu was involved in this murder-for-hire conspiracy, along with Eratay, Aron Ethridge, and Jerry Banks. Davis's murder involved the following federal crimes: kidnapping, in violation of 18 U.S.C. § 1201, murder to obstruct justice, in violation of 18 U.S.C. § 1512(a)(1); murder for hire, in violation of 18 U.S.C. § 1958; and wire fraud, in violation of 18 U.S.C. § 1343. There is probable cause to believe that the SUBJECT DEVICE contains evidence of those crimes, as described in Attachment B.

4. This case is being investigated by the FBI and the Vermont State Police (VSP). Since this affidavit is being submitted for the limited purpose of establishing probable cause to search data already in law enforcement's custody, I have not included details of every aspect of the investigation. Except as otherwise noted, the information contained in this affidavit is based upon my personal knowledge and observations, my training and experience, conversations with other law enforcement officers and witnesses, and my review of documents and records.

Probable Cause

5. On April 29, 2022, I obtained a search warrant for a computer hard drive seized during a search at Jerry Banks' Colorado residence. A copy of my affidavit submitted in support of the search warrant is attached as Exhibit 1. Its contents remain true and correct, and I incorporate those contents here.

6. As set forth in more detail in Exhibit 1, there is probable cause to believe that prior to his murder, Davis was the victim of a financial fraud scheme involving Serhat Gumrukcu and his brother, Murat Gumrukcu. This financial fraud scheme involved false statements by the Gumrukcus about their ability to provide funding to support investments in an oil trading company, as described in agreements between the Gumrukcus' company, Lauran Trading, LLC; Gregory Davis's company, Mode Commodities, LLC; and Gregory Gac's company, Quadrant Financial Group, LLC (functioning as an "escrow agent" for the parties). Exhibit 1 contains evidence about Davis's complaints about the Gumrukcus' alleged fraud and Davis's threats to report the Gumrukcus' fraud to the FBI during the second half of 2017. My review of Davis's text messaging with Gac and Gac's text messaging with Serhat Gumrukcu show that Davis was alleging fraud by the Gumrukcus as early as late 2015. Davis's complaints continued in 2016 and early 2017. During this two-year period, Serhat Gumrukcu made various claims to Gac about his ability and plans to complete the funding for Mode Lauran. Gumrukcu never came up with the Letter of Credit funding contemplated by the Mode Lauran agreements. Davis complained through Gac repeatedly about the falsity of Gumrukcu's claims. Gregory Davis used the nickname "Gregg" not "Greg."

7. As set forth in Exhibit 1, there is probable cause to believe that Jerry Banks murdered Davis, and that he was hired to do so on behalf of a third party. As set forth in Exhibit 1, the only known link between Banks and the Gumrukcus was Aron Ethridge and Berk Eratay.

8. On April 6, 2022, Jerry Banks was arrested in Yellowstone National Park. The arrest generated substantial media attention.

9. On April 7, 2022, I interviewed Aron Ethridge near his home in Henderson, Nevada. During this initial interview, Ethridge denied all knowledge of a murder-for-hire scheme involving Banks. On the morning of April 9, 2022, I received a call from Ethridge, who agreed to meet again later that day. At this second meeting, Ethridge admitted he had lied during the first meeting, and then confirmed the murder-for-hire scheme involving Banks, Eratay, and Gumrukcu. A third meeting with Ethridge was held on April 10, 2022, during which Ethridge admitted he had omitted some of his knowledge of the plan to abduct Davis during his interview on April 9. The following is a summary of the information that Ethridge provided to law enforcement during the April 9 and April 10 interviews, with corrections as provided by Ethridge on April 10:

a. Ethridge and Eratay used to be neighbors in Henderson, Nevada, and became friends during that period.

b. Eratay approached Ethridge over a year before the murder of Davis, asking if Ethridge could arrange a murder. Ethridge eventually agreed to assist Eratay.

c. Ethridge approached Banks, asking Banks to assist with the murder.

d. Ethridge received over $110,000 in cash from Eratay as payment for the murder. A portion of this cash was paid to Banks.

e. The initial plan had been for Banks to "snipe" Davis, but after Banks made a reconnaissance trip to Vermont, Banks advised the plan would have to be revised and requested additional payment due to the increased difficulty of the job.

f. Ethridge knew that Banks would impersonate a law enforcement officer and abduct Davis from his residence prior to murdering him.

g. Ethridge and Banks communicated via an encrypted application called "Threema." Ethridge also communicated with Eratay on the "Threema" application.

h. On at least one occasion, Banks used a physical data card to pass along a digital image of Davis that Banks had taken during a trip to Vermont. Ethridge provided this data card to Eratay.

i. On January 7, 2018, while Banks was traveling back from Vermont, Banks called Ethridge and advised him the job was done. Ethridge then called Eratay to relay the message.

j. Ethridge had met Serhat Gumrucku on multiple occasions prior to the murder of Davis. Ethridge believed that, based on these meetings and statements made by Eratay, Serhat was the man who wanted Davis killed. Eratay told Ethridge that Serhat had a problem with Davis and asked Ethridge to help them get rid of the problem. However, Serhat and Ethridge never directly communicated about the abduction and murder. All communications went through Eratay, who Ethridge knew to work for Serhat.

k. After the murder of Davis, Eratay provided Ethridge with an additional payment in the form of Bitcoin.

l. Eratay attempted to contact Ethridge in early April after Ethridge and Eratay were separately contacted by federal agents.

10. FBI Special Agent Christopher McPeak interviewed Eratay on April 7, 2022. I have spoken with Agent McPeak and reviewed the report summarizing the interview. Eratay denied knowing anything about Davis or his oil deal with the Gumrukcus. Eratay admitted the Gumrukcu brothers are family friends from Turkey. Eratay stated that he had done IT work for companies involving Serhat Gumrukcu, including Enochian Biosciences. He admitted to various financial transactions with Serhat Gumrukcu but initially denied receiving transfers totaling over $30,000. When agents noted that they had seen the transfers described above, Eratay said that Gumrukcu was repaying him for prior medical expenses loaned to Gumrukcu by Eratay's father.

Eratay also said that Serhat Gumrukcu gave him Enochian stock, which Eratay estimated to be be worth approximately $100,000.

11. I have reviewed some of the contents of the berkeratay@gmail.com account, used by Eratay. Data from July 27, 2017 has a subject line of "Person's Details." This data appears to reflect Google's capture of an Apple Note, which is an Apple application that allows users to wrote notes on an Apple device, including an iPhone. The body of the "Note" reads as follows:

> Person's Details;
>
> Gregory Charles Davis
>
> Birth Date: 27 Oct 1968
>
> Place Of Birth: NJ USA
>
> His Company Name is Mode Commodities LLC:
> 101 Hudson Street
> Jersey City NJ 07302
>
> Gregg's cell is +1 802 377 1303

Based on my investigation, this "Note" accurately captures Davis's middle name and date of birth. Thus, I believe that Eratay was provided with details about Davis for purposes of the murder-for-hire conspiracy.

12. I have reviewed bank records of Serhat Gumrukcu and Berk Eratay obtained by grand jury subpoena. Between May 2017 and October 2017, Gumrukcu transferred approximately $200,000 from a Turkish bank account to U.S. accounts controlled by Eratay. During those same months, Eratay withdrew the bulk of those funds in cash, regularly withdrawing funds in amounts of $9,000, an amount below the $10,000 currency reporting trigger.

13. I have reviewed some of the contents of the Google account serhat.gumrukcu@gmail.com, used by Serhat Gumrukcu. Records of chats from the serhat.gumrukcu@gmail.com account reveal chats with the berkeratay@gmail.com as far back as 2014 and include discussions of Paypal transactions. The contents of the serhat.gumrukcu@gmail.com email account reveal that Eratay has been involved in assisting Serhat with his business ventures since at least the summer of 2015. These business ventures reflect that Eratay is involved in coordinating and arranging investment discussions between Serhat and others. They also reflect that Eratay assisted Serhat in arranging for personal transactions.

14. On May 24, 2022, Eratay was arrested outside his residence in Las Vegas, Nevada. At the time of his arrest he did not possess a cell phone. On June 16, 2022, I went to Eratay's Las Vegas residence to interview HK, a friend of Eratay's, and to serve him with a grand jury subpoena. During the interview, HK told me that Eratay gave him custody of the SUBJECT DEVICE after Eratay's arrest, that HK had changed the password on the device, and that HK was using it with Eratay's permission to conduct certain financial transactions on Eratay's behalf. HK turned over the phone to me pursuant to the grand jury subpoena. HK also told me that Eratay had told him that he and Serhat Gumrukcu were close, that they worked together in the past, and that they had been working more closely together more recently. HK also said that Eratay told him that he was in communication with Gumrukcu after Eratay was interviewed by the FBI in April 2022.

15. On May 24, 2022, Serhat Gumrukcu was arrested in Los Angeles, California. Agents seized a phone and a laptop at the time of Gumrukcu's arrest. On June 10, 2022, I obtained a search warrant to search the Gumrukcu devices based on the information described in this affidavit.

16. My review of Gumrukcu's text messages with Gac from 2017 and a review of Gumrukcu's email account, obtained by search warrant, show that during 2017, while the murder plot was pursued, Gumrukcu was putting together a financial transaction creating Enochian Bioscience. Enochian Bioscience was created out of a merger between Enochian Biopharm, which Gumrukcu controlled, and DanDrit Bioscience, a publicly traded company owned and controlled by third parties. I have reviewed SEC submissions showing that the Enochian merger closed in January 2018, soon after the murder. Shortly thereafter in early 2018, Enochian Bioscience began trading on the NASDAQ. As a result of the merger deal, Gumrukcu and his spouse controlled a majority of the shares in Enochian Bioscience. Those shares had a market value of approximately $100 million in early May 2022. The SEC filings and publicly available internet information show that Gumrukcu maintained active involvement in Enochian up to the time of his arrest.

17. During 2017, Gumrukcu faced felony fraud charges prosecuted by the State of California. He was arrested in early 2017 and charged by complaint with two fraud schemes. The first involved evidence that Gumrukcu obtained approximately $1 million from a Turkish investor to buy and renovate a Los Angeles residential property for resale. According to the FBI agent who participated in the investigation, Gumrukcu did not buy or renovate the property with the funds he obtained from the investor; Gumrukcu spent the funds on other expenses; and Gumrukcu submitted false and forged documents to the investor to cover up his embezzlement. The second fraud scheme involved bounced checks written by Gumrukcu to Gac in May 2016 to pay fees and penalties for the Mode Lauran deal with Gregory Davis. Gumrukcu wrote checks totaling $600,000 on an account that had a negative balance at the beginning and end of May 2016. The California court held a probable cause hearing on the Gumrukcu charges in October 2017 and found probable cause for all the charges. The California prosecutor then filed an information containing those charges. In early January 2018, shortly after the murder, Gumrukcu

pleaded guilty to a single felony charge and was sentenced to five years of probation. In 2020, Gumrukcu successfully had the charge amended to a misdemeanor under California law.

18. Based on the information above, I believe that there is probable cause that the Enochian deal played a role in the motive for the murder for hire. Based on my training and experience, I believe that the SUBJECT DEVICE contains information about Eratay's business and financial relationships involving Enochian.

19. Based on the information above, as well as my training and experience, I believe it is likely that Eratay communicated with other co-conspirators about the developments in the Davis murder investigation after Banks was arrested and Eratay was interviewed. Moreover, I believe that there is probable cause that the SUBJECT DEVICE contains evidence about those communications.

Electronic Storage and Forensic Analysis

20. Based upon my training and experience, and my discussions with other law enforcement officials, I know the following:

a. Users of digital devices increasingly choose to store items in digital form (e.g. pictures or documents) because digital data takes up less physical space, and can be easily organized and searched. Users also choose to store data in their digital devices because it is more convenient for them to access data in devices they own, rather than to later spend time searching for it. Keeping things in digital form can be safer because data can be easily copied and stored off site as a failsafe.

b. Users also increasingly store things in digital form because storage continues to become less expensive. Today, one terabyte (TB) hard drives are not uncommon in computers. As a rule of thumb, users with one gigabyte of storage space can store the equivalent of 500,000 double spaced pages of text. Thus, each computer can easily contain the equivalent of 500 million pages, that, if printed, would fill six 35' x 35' x 10' rooms. Similarly, a one TB drive could contain 900 full run movies, or 900,000 songs, or four million images. With digital devices, users can store data for years at little cost to no cost.

c. Storing data in digital form and not deleting it mirrors users' online habits where users have, for many years, been encouraged to never delete their emails. For example, since June 2007, Google, Inc. has promoted free, increasingly larger storage "so you should never have to delete mail." *See* Bill Kee, *Welcome to Official Gmail Blog*, https://gmail.googleblog.com/2007/06/welcome-to-official-gmail-blog.html (July 3, 2007); *see also* Rob Siembroski, *More Gmail Storage Coming For All*, https://gmail.googleblog.com/2007/10/more-gmail-storage-coming-for-all.html (Oct. 12, 2007) (promoting its "Infinity+1" plan to constantly give subscribers more storage).

d. Digital devices can also store data automatically, without a user's input. For example, network logs may track an employee's actions for company auditing purposes or email headers may automatically list the servers which transmitted the email. Similarly, a web browser (i.e. an application such as Internet Explorer used to access web pages) can track a user's history of websites visited so users can more easily re-access those sites. Browsers also temporarily cache files from recently accessed web pages to improve the user's experience by reducing that page's loading time. These examples illustrate how the interaction between software and operating systems often results in data being stored without a user's knowledge. Even if a sophisticated user understands this automatic storage of data, attempts at deleting this data often fail because the data may be automatically stored multiple times and in different locations. Thus, digital evidence may exist despite attempts at deleting it.

e. Digital data is practically resilient to deletion. First, as noted, data is often automatically stored multiple times in multiple locations, where even sophisticated users may not be able to locate. Second, digital data can be recovered years after it has been saved, or viewed even after such data has been deleted. For example, when a user deletes a file on a computer, the file is sent to the recycle bin, where it can still be retrieved. Even if the file is deleted from the recycle bin, the data does not actually disappear; rather it remains in "free space" or "slack space" (i.e. in unused space) until it is overwritten by new data. Third, an operating system may also keep deleted data in a "recovery" or "swap file." Fourth, files from websites are automatically retained in a temporary cache which is only overwritten as they are replaced with more recently viewed web pages. Thus, the ability to retrieve residues of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer use habits.

21. Based on my training, my experience, and information provided to me by those involved in the forensic examination of digital devices including cell phones, I know that completely segregating information before an examiner has started reviewing digital evidence is inconsistent with the evidence assessment process. This is true for the following reasons:

a. This application seeks permission to locate and seize not only data that might serve as direct evidence of the Subject Offenses, but also for evidence that establishes how digital devices were used, the purpose of their use, and who used them. Additionally, this application seeks information about the possible location of other evidence.

b. This application seeks permission to search and seize evidence, fruits, or instrumentalities found in the devices described in Attachment A. Some of these items may be files and other data that is generated by a user (e.g. documents, pictures, and videos). Alternatively, other items may be device generated data that becomes meaningful only upon forensic analysis. For example, as noted, a hard drive may contain records of how a computer was used, the purposes for which it was used, and who has used these records. These items are the subject of this warrant.

c. For instance, based upon my training, my experience, and information provided by others involved in the forensic examination of digital devices, I know the following: First, as noted, data that is not currently associated with any file can provide evidence of a file that once existed, but which has since been deleted or altered. This can include a deleted portion of a file (e.g. a paragraph deleted from a document). Second, applications such as web browsers, email, and chat programs store configuration information that can reveal information such as online nicknames and passwords. Third, operating systems can record information, such as the attachment of peripherals (e.g. USB flash drives), and the times the device was in use. Similarly, file systems record the dates files were created and the sequence in which they were created. Any of this information may be evidence of a crime, or indicate the existence and location of evidence in other locations on the digital device.

d. In determining how a digital device has been used, the purpose for which it was used, and who has used it, it is sometimes necessary to establish that a particular thing is not present. For example, in cases where more than one person has used a digital device, agents can infer that a defendant must have been the person who used that device to commit a crime by eliminating the possibility that other people used that device during that time. Because file systems often list the dates and times those files were created, this information can help exclude the possibility that other people were using that digital device. As another example, by reviewing a computer's Index.dat files (a system file that keeps track of activity conducted in Internet Explorer), a forensic examiner can determine whether a user accessed other information close in time to the file creation dates, times, and sequences so as to establish user identity and exclude others as having used that computer during times related to the criminal activity. Demonstrating the significance of the absence of certain data on a digital device may require analysis of the digital device as a whole.

e. The types of evidence described above may be direct evidence of a crime, indirect evidence of a crime indicating the location of evidence or a space where evidence was once located, contextual evidence identifying a user or excluding a user. All of these types of evidence may indicate ownership, knowledge, and intent.

f. This type of evidence is not "data" that can be segregated, that is, this type of data cannot be abstractly reviewed and filtered by a seizing or imaging agent and then transmitted to investigators. Rather, evidence of this type is a conclusion, based on a review of all available facts and the application of knowledge about how a computer behaves and how computers are used. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

22. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all emails within the Subject Account. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other

methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

23. Based on my training, my experience, and information given to me by others involved in the forensic examination of digital devices, I know that searching for this kind of evidence involves technical, complex, and dynamic processes, which may require expertise, specialized equipment and a knowledge of how digital devices are often used to commit the Subject Offenses.

24. There is probable cause to believe that things that were once stored on the SUBJECT DEVICE may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

25. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

26. The SUBJECT DEVICE has been stored in such a manner that the data on it likely remains in the same condition as when law enforcement first seized it.

27. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

28. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41. The proposed search warrant would authorize the government to conduct a forensic examination of the SUBJECT DEVICE. Because the government already has custody of the SUBJECT DEVICE, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

Dated at Burlington, in the District of Vermont, this 7th day of July 2022.

Patrick Hanna
Special Agent - FBI

Sworn to and subscribed before me this 7 day of July 2022.

Honorable Geoffrey W. Crawford
United States District Judge